

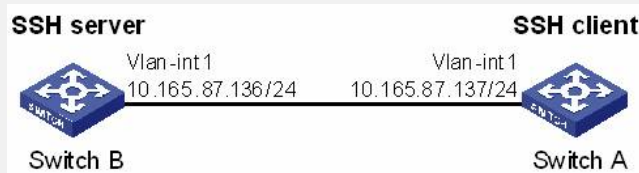
S2000-EA系列交换机充当SSH客户端并采用公钥认证功能的配置

一、组网需求：

当用户通过交换机远程登录到另一台交换机时，如果通过的网络不能保证安全，为更最大限度地保证数据信息交换的安全性，使用SSH来实现此目的，并采用公钥认证。如下图所示：

- (1) 交换机Switch A作为SSH客户端，用来进行SSH登录的用户名为client001。
- (2) 交换机Switch B作为SSH服务器，IP地址为10.165.87.136。

二、组网图：



三、配置步骤：

1、配置SwitchB

在交换机上创建VLAN接口，并为其分配IP地址，作为客户端连接的SSH服务器地址。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

生成RSA和DSA密钥对。

```
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
```

设置用户接口上的认证模式为AAA认证。

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

设置用户接口上支持SSH协议。

```
[SwitchB-ui-vty0-4] protocol inbound ssh
```

设置用户能访问的命令级别为3。

```
[SwitchB-ui-vty0-4] user privilege level 3
[SwitchB-ui-vty0-4] quit
```

创建用户client001，并指定认证方式为公钥认证。

```
[SwitchB] ssh user client001 authentication-type publickey
```

这里需要先在SSH客户端生成DSA密钥对，并将生成的DSA公钥保存到指定文件中，再将此公钥文件通过FTP/TFTP方式上传到服务器端，文件名为Switch001。

在服务器端从文件Switch001中导入客户端的公钥，公钥名为Switch001。

```
[SwitchB] public-key peer Switch001 import sshkey Switch001
```

为用户client001指定公钥Switch001。

```
[SwitchB] ssh user client001 assign publickey Switch001
```

2、配置SwitchA

在交换机上创建VLAN接口，并为其分配IP地址，作为连接SSH服务器端的SSH客户端地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

生成DSA密钥对。

```
[SwitchA] public-key local create dsa
```

将生成的DSA主机公钥导出到指定文件中，文件名为Switch001。

```
[SwitchA] public-key local export dsa ssh2 Switch001
```

客户端生成密钥对后，需要将保存的公钥文件通过FTP/TFTP方式上传到服务器端，并完成服务器端配置后，才可继续客户端的配置。

建立到服务器10.165.87.136的SSH连接。

```
[SwitchA] ssh2 10.165.87.136 identity-key dsa
```

```
Username: client001
```

Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n

* Copyright(c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved.*
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *

四、 配置关键点:

采用公钥认证时，可以采用RSA或DSA公钥作为服务器端认证客户端的公钥。这里以DSA公钥为例。生成服务器端的RSA和DSA密钥对是完成SSH登录的必要操作。